KRYPTODISK 2

SSD

Capacity
128GB, 256GB, 512GB, 1TB

Interface
USB 3.1

Operating System
Linux, Windows and Mac

Package includes
KryptoDisk
USB cable
Quick installation guide
Smart card

Models

KryptoDisk | Selfkey (B,S)
KryptoDisk | User primary and user data restore
KryptoDisk | KMS

Product features

KryptoDisk – Selfkey (B,S)
This is the ideal product if you want to be in control of your data, PIN and PUK.

KryptoDisk user primary and user data restore
With this solution you have an extra set of cards with PIN/PUK that you can keep in a safe place in case your key card is lost or stolen.

KryptoDisk KMS
By replacing the Hiddn "Selfkey" smart card with a managed smart card the IT department can keep control of keys, units and users.

Enabling a safe USB environment
KryptoDisk is the perfect solution for transportation of data between the office and home, for travelling with sensitive data, for working between office branches and for moving sensitive data between systems and platforms.

Easy to use
KryptoDisk comes with a bright, easy to read OLED display that informs the user about the status of the device.

Plug and Play
KryptoDisk can be used straight out of the box and does not require any software or drivers to be installed prior to use. It is compatible with various operating systems (OS). Before first time use you will need to format the KryptoDisk. Our installation guide will guide you through this process.

Product features

Two-factor authentication
The smart card and the secret passphrase are the two factors required to be granted access to the data. Something you have and something you know – the same security level commonly used for access your bank account.

Key management system
With KryptoDisk KMS the administrator can define authentication policies and facilitate key escrow.

Bootable secure environment
KryptoDisk operates either as a generic external storage or as a bootable external disk. A secure bootable disk make it possible to use virtually any computer and still operate in a secure environment.

Security features

Data Recovery
An unfortunate user entering the wrong PIN/passphrase too many times does not have to face erased data, but may still recover from the situation of a locked storage device by entering the PUK.

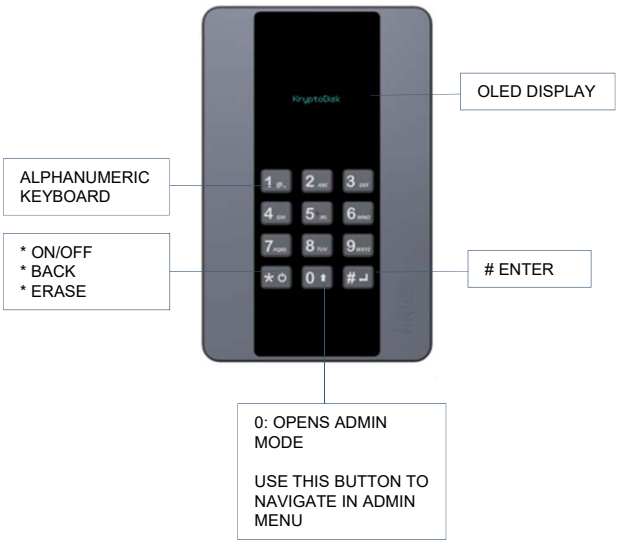
Authentication
Users can change PIN/PUK. A PUK can reopen the smart card and the user can set a new PIN/PUK. To many failed attempts to enter PUK will permanently lock the smart card and erase all data.

Password attack protection
All data encryption keys are stored in Common Criteria EAL + certified tokens (smart cards).

Technical Specifications

Encryption algorithm	AES-256
Interface	USB 3.1
Approvals	FIPS 140-2 LEVEL 3
Capacities	128 GB, 256 GB, 512 GB, 1TB
Authentication mode	7-16 digit PIN + smart card
Read / Write	✓
Tamper-proofed	✓
Brute-force defense	✓
2-factor authentication	✓
Bootable	✓
Resistant to keyloggers	✓
Encryption key stored separately	✓
Transfer speed	80 MB/s

Functions



Hiddn's advantage

Designed, produced and assembled in Norway

Support
www.hiddn.no/support

sales@hiddn.no